Statewide Security Manual and Glossary Changes
Fall 2008

The State Chief Information Officer has approved the following changes and additions to the Statewide Information Security Manual and the State Information Technology policies as a result of his annual review and revision of the standards, as required by G.S. § 147-33.110. Statewide security standards.

The changes are underlined. The versions that are included in the Statewide Information Security Manual and the individual chapters are not underlined although the changes are noted at the end of each chapter, where applicable. For questions, please contact Ann Garrett, State Chief Information Security Officer at 919-754-6300 or at Ann.Garrett@its.nc.gov.

SECTION I – Insertion of Existing Policies into Manual

The standards listed in this section include parts of other policies and standards that were not included in the Statewide Information Security Manual ("Manual") but were part of other policies and standards maintained by the State Chief Information Officer on the Statewide IT Policies and Standards page, under "Other Security Standards and Policies." When the Manual was originally written, most of the material in the existing policies and standards was included in the Manual. The parts that were not included at that time have been inserted into the Manual, where appropriate.

The additions are underlined. The footnotes indicate the source of the language.

010101 Defining Information

Purpose: To protect the State's information.

STANDARD[1]

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any agency of State government.

The State's information shall be handled in a manner that protects the information from unauthorized or accidental disclosure, modification or loss. All agencies shall maintain a comprehensive and up-to-date database of their information assets and periodically review the database to ensure that it is complete and accurate.

Each agency, through its management, is required to protect and secure the information assets under its control. The basic information requirements include, but are not limited to:

- Identifying information assets and maintaining a current inventory of information assets.
- Complying with applicable federal and state laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Assessing the vulnerability and risk associated with information assets.
- Determining the value of information assets to the organization and the business processes they support.
- Providing the level of information protection for information assets that is appropriate to their vulnerability, risk level, and organizational value.
- Maintaining a business and disaster recovery plan with respect to information technology and process.

ISO 27002 REFERENCE

7.2.1 Classification guidelines

[1] From the Information Protection Asset Policy

010103 Storing and Handling Classified Information

Purpose: To protect the State's information, including information security records, through the establishment of proper controls.

STANDARD[2]

The State's information, data and documents shall be handled in a manner that will protect the information, data and documents from unauthorized or accidental disclosure, modification or loss. All information, data and documents must be processed and stored in accordance with the classification levels assigned to those data in order to protect their integrity, availability and, if applicable, confidentiality.

The type and degree of protection required shall be commensurate with the nature of the information, the operating environment, and the potential exposures resulting from loss, misuse or unauthorized access to or modification of the data.

An agency that uses confidential information from another agency shall observe and maintain the confidentiality conditions imposed by the providing agency, if legally possible.[3]

Special protection and handling shall be provided for information that is covered by statutes that address, for example, the confidentiality of financial records, taxpayer information and individual census data.

The State CIO shall manage and protect confidential information technology security records that agencies provide to his office and the Office of Information Technology Services (ITS). The records submitted to the State CIO or ITS that are confidential because the records disclose information technology security features shall so designate the records by affixing the following statement, "Confidential per G.S. §132-6.1(c)", on each page.

Confidential information technology security records shall be provided only to agencies and their designated representatives when necessary to perform their job functions.

Confidential information technology security records shall not be transmitted electronically over ~~open~~ public[4] networks unless encrypted while in transit.[5]

Employees who are provided access to information technology security records shall sign a non-disclosure agreement that includes restrictions on the use and dissemination of the records. Agencies shall ensure that legal and business risks associated with contractors' access are determined, assessed and appropriate measures are taken. Such measures may include, but are not limited to, non-disclosure agreements, contracts, and indemnities.

---

[2] Added "Confidential Security Information Policy."

[3] *See*, News and Observer v. Poole, 330 N.C. 465, 412 S.E.2d 7 (1992).

[4] For the purpose of this standard, a public network includes the State Network. It does not apply to internal agency networks.

[5] Encryption is defined in the Security Architecture Chapter, Standard 3 "Use Cryptography based on Open Standards."

GUIDELINES

An appropriate set of procedures should be defined for information labeling and handling in accordance with the classification scheme adopted by the agency. The procedures should cover information assets in both physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information-processing activity:

- ❑ Copying
- ❑ Storage
- ❑ Transmission by post, fax, and electronic mail
- ❑ Transmission by spoken word, including mobile phone, voice mail, and answering machines

- Output from systems containing information that is classified as confidential or critical should carry an appropriate classification label. The labelling should reflect the classification according to the rules established by Standard 010102, Setting Classification Standards—Labelling Information. Items for consideration include printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, cassettes, USB flash memory drives), electronic messages and file transfers.
-
- Where appropriate, physical assets should be labelled. Physical labels are generally the most appropriate forms of labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling need to be used. In other cases, such as with tapes, a physical label is appropriate for the outside of the tape in addition to electronic labelling of documents contained on the tape.
-
- The originator of a telephone call, a telex/cable, a facsimile transmission, an email, a computer transaction, or any other telecommunications transmission should be aware of the possibility of compromise of confidentiality or integrity of the information transmitted and determine whether the information requires additional special protection and handling.

RELATED INFORMATION
Standard 010107 Setting Classification Standards—Managing Network Security

ISO 27002 REFERENCE
10.7.3 Information handling procedures

020102 Managing User Access

Purpose: To prevent unauthorized access to agency networks.

STANDARD[6]

Agencies shall be responsible for establishing a procedure for managing access rights for users of their networks throughout the life cycle of the user ID. Agencies

[6] Added pieces of User ID and Password Protection Standard that had not been incorporated at an earlier time.

shall identify a backup system administrator to assist with user ID management when the primary system administrator is unavailable.

Only authorized users shall be granted access to State information systems. Users shall be responsible for maintaining the security of their user IDs and passwords. User IDs shall be individually assigned in order to maintain accountability. Each user ID shall be used by only a single individual, who is responsible for every action initiated by the account linked to that user ID. Where supported, the system shall display (after successful login) the date and time of last use of the individual's account so that unauthorized use may be detected.

User IDs shall be disabled promptly upon a user's termination from work for the State or upon cessation of a user's need to access a system or application. User IDs that are inactive for 30 days must be disabled, except as specifically exempted by the security administrator.

Only authorized system or security administrators and service desk staff shall be allowed to enable or re-enable a user ID except in situations where a user can do so automatically through challenge/response questions or other user self service mechanisms.

Logging of Administrator Activity

All user ID creation, deletion and change activity performed by system administrators and others with privileged user IDs shall be securely logged and reviewed on a regular basis.

Concurrent Connections

For those systems that enforce a maximum number of concurrent connections for an individual user ID, the number of concurrent connections must be set to two (2).

Outside User IDs

User IDs established for a nonemployee/contractor must have a specified expiration date unless the provision of a user ID without a specified expiration date is approved in writing by the agency security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.

Access control may need to be modified in response to the confidentiality of information contained on the system, if existing access controls pose a risk that confidentiality may be breached.

ISO 27002 REFERENCE
11.2User access management

020104 Managing Network Access Controls

Purpose: To establish requirements for the access and use of the State Network and agency networks.

STANDARD[7]

Access to networks operated by State agencies, including the State Network, shall be controlled to prevent unauthorized access and to prevent malicious attacks on the networks. Access to all agency computing and information systems shall be restricted unless explicitly authorized.

- All remote access (dial-in services) to the networks shall be either through an approved modem pool or via an Internet service provider (ISP).
- Remote users shall connect to the State Network only using protocols approved by the State Chief Information Officer (State CIO). Remote users with direct connections to agency networks shall follow agency protocols.
- When users on the agency networks connect to external systems, including the State Network, they shall comply with Standards 030303 – Sending Electronic Mail and 100301 – Using the Internet in an Acceptable Way.
- Users on the State Network shall not be connected to the State Network at the same time as they are using a modem to connect to an external network.
- Users shall not extend or retransmit network services in any way without appropriate management approval.
- Users shall not install network hardware or software that provides network services, such as routers, switches, hubs and wireless access points, without appropriate management approval.
- Non–State of North Carolina computer systems that require connectivity to the State Network shall conform to statewide security standards.
- Non–State of North Carolina computer systems that require connectivity to agency networks shall conform to agency security standards.
- Users shall not download, install or run security programs or utilities that reveal weaknesses in the State Network without prior written approval from the State CIO.
- Users shall not download, install or run security programs or utilities that reveal weaknesses of agency networks without appropriate agency management approval. For example, State users must not run password-cracking programs, packet sniffers, network-mapping tools or port scanners while connected in any manner to the State Network infrastructure. Users shall not be permitted to alter network hardware in any way.

ISO 27002 REFERENCE
Network access control

[7] Added material from the “Remote Access Security Standard”

020106 Managing Passwords

Purpose: To prevent unauthorized access and to establish user accountability when using IDs and passwords to access State information systems.

STANDARD [8]

Agencies shall manage passwords to ensure that all users are properly identified and authenticated before being allowed to access State information systems. The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to an information system when IDs and passwords are selected as the method of performing identification and authentication. A unique user ID shall be assigned to each user so that individual accountability can be established for all system activities. Management approval shall be required for each user ID created. A process shall be in place to remove, suspend or reassign user IDs that become inactive as a result of employee or contractor movements.

The system's authentication system shall limit unsuccessful logon attempts. Where possible, unsuccessful logon attempts shall be limited to three before the user logon process is disabled. Information shall be maintained on all logon attempts to facilitate intrusion detection.

Password management capabilities and procedures shall be established to ensure secrecy of passwords and prevent exploitation of easily guessed passwords or weaknesses arising from long-life passwords. Each agency shall evaluate its business needs and the associated risks for its information systems in conjunction with identification and authentication requirements. When IDs and passwords are selected as the method of performing identification and authentication, agencies are required to select and use the appropriate standards and best practices. Agencies must specify the minimum requirements for identification and authentication using IDs and passwords in accordance with the standard criteria that follow. Depending on the operating environment and associated exposures, additional or more stringent security practices may be required.

- For secured access to systems and applications that require a low level of security, passwords shall have at least six (6) characters of any sort.
-
- For access to all systems and applications that require a high level of security, such as electronic fund transfers, taxes and credit card transactions, passwords shall be at least eight (8) characters.
-
- To the extent possible, passwords shall be composed of a variety of letters, numbers and symbols with no spaces in between[9].
-
- To the extent possible, passwords shall be random characters from the required categories of letters, numbers and symbols.
-
- Passwords shall not contain dictionary words or abbreviations.

[8] Inserts from Section 3.22 from the User ID and Password Protection Standard.

[9] For Resource Access Control Facility (RACF), valid symbols are @, $, #, and _, and the first character of a password must be a letter and the password must contain a number.

- Passwords shall not contain number or character substitutes to create dictionary words (e.g., *d33psl33p* for *deep sleep*[10]).
- Passwords for internal State resources shall be different from passwords for external, non-State resources.
- Password generators that create random passwords shall be allowed.
- Password management application features that allow users to maintain password lists and/or automate password inputs shall be prohibited, except for simplified/single sign-on systems approved by the State Chief Information Officer (State CIO).

Password Management Standards

- Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including supervisors, family members or co-workers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.
- Users shall enter passwords manually, except for simplified/single sign-on systems that have been approved by the State CIO.
- No automated password input shall be allowed, except for simplified/single sign-on systems that have been approved by the State CIO.
- Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media. If stored, passwords shall be stored in encrypted format.
- Password Changes: Government employees and contractor password (e.g., email, Web and calendar) used to access systems and applications shall be changed at least every ninety (90) days. Passwords shall not be reused until six additional passwords have been created.
- Passwords for citizens and business users do not need to be changed; use of strong passwords and periodic password changes, however, are recommended.
- Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established.
- Where possible and practicable, access to password-protected systems shall be timed out after an inactivity period of thirty (30) minutes or less or as required by law, if the inactivity period is shorter than thirty (30) minutes.
- Passwords shall not be displayed in clear text during the logon process or other processes. Where possible, applications that require clear-text authentication shall be converted to equivalents that can use encryption.[11]

[10] Other examples of numbers/symbols for letters are *0* for *o*, *$* or *5* for *S*, *1* for *i*, and *1* for *l*, as in *capta1n k1rk* or *mr5pock*.

[11] Encryption is defined in the Security Architecture Chapter, Standard 3, Use Cryptography Based on Open Standards.

- Passwords shall be changed whenever there is a chance that the password or the system could be compromised.

Password Management Standards—System Administrators

- All passwords (e.g., Unix, NT and RACF) shall be changed at least every ninety (90) days. Passwords for administrative user accounts and accounts with special privileges shall be changed at least every thirty (30) days.
-
- A user account that has system-level privileges or programs such as root access shall have a different password from all other accounts held by that user.
-
- Password files shall be retrievable only by the security administrator or a designated backup security administrator.
-
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset as soon as an information system is installed.
-
- The password for a shared administrative-access account shall change when any individual who knows the password leaves the agency that established the account or when job responsibilities change.
-
- In situations where a system has only one administrator, agencies shall establish a password escrow procedure so that, in the absence of the administrator, someone can gain access to the administrator account.

ISO 27002 REFERENCES

11.2.3	User password management
11.3.1	Password use
11.5.1	Secure log-on procedures
11.5.2	User identification and authentication
11.5.3	Password management system

030101 Configuring Networks and Configuring Domain Name Servers (DNS)

Purpose: To establish a framework for the configuration of networks and domain name servers.

STANDARD[12]

Agency network infrastructures shall be designed and configured using controls to safeguard the State's information systems. Failure to protect network infrastructures against threats can result in the loss of data integrity, data unavailability and/or unauthorized data use. Secure configuration of the network infrastructure shall include but not be limited to the following:

- All hardware connected to the State Network shall be configured to support agency management and monitoring standards.
- The cabled network infrastructure must comply with industry standards and be installed by a licensed, bonded contractor.

[12] The DNS Security Standard has been added at the end.

- Perimeter defense systems, including routers and firewalls, and network-connected equipment, including switches, wireless access points, personal computers and servers, shall be configured to secure specifications approved by security institutes such as the SANS Institute or the National Security Agency (NSA).
- All network address space (Internet Protocol [IP]/Internet Packet Exchange [IPX]) shall be distributed, registered and managed by ITS.
- Critical hardware and systems, including the network infrastructure, shall be connected to an uninterruptible power supply (UPS).
- Network devices shall be configured to support authentication, authorization and accountability mechanisms when being administered.
- Configuration management, patch management and change management standards and procedures shall be applied to all applicable systems.
- Extending, modifying or retransmitting network services, such as through the installation of new switches or wireless access points, in any way is prohibited, unless prior approval is granted.
- Configuration shall include elimination of the possibility of bridging networks via secondary Internet connections.
- Network servers/services such as email, Web, and ftp shall be segregated from an agency's internal user LAN.
- Configuration shall include accommodations for flexibility, scalability and reliability to meet growing user demands and conserve IT funds of the future.

No DNS server can be configured to allow zone transfers to unknown secondary servers.

- If an agency maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers.
- If an agency maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only.
- When a domain has a US extension (*i.e.,* state.nc.us), the US Domain Registry requires that the domain allow copies to be transferred to the US Domain Registry's Master Server. Therefore, all domains registered with US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry.
- When ITS maintains the DNS, agencies may request ITS to allow additional IP addresses to receive zone transfers. Agencies must work with ITS to define acceptable IP addresses and/or IP address ranges.

ISO 27002 References

10.6 Network security management
11.4 Network access control
11.4.2 User authentication for external connections

030107 Routing Controls, including Firewall Configuration

Purpose: To protect access to the State's routed networks.

STANDARD[13]

Agencies shall deploy mechanisms to control access to the State's network backbone and/or routed infrastructure. Protective controls shall at a minimum include the following:

- Positive source and destination address checking to restrict rogue networks from manipulating the State's routing tables.
- Authentication to ensure that routing tables do not become corrupted with false entries.
- Network address translation (NAT) to screen internal network addresses from external view.
- Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to accomplish the mission of the agencies.

Firewall Configuration and Installation

1. Default: The default firewall policy is for all ports to be closed. Only those ports for which an agency has written, documented business reasons for opening shall be open. Each agency shall establish a process for evaluating policy changes that, at a minimum, incorporates requirements for compliance to the security matrix for communications across trust levels and emphasizes alternative methodologies to achieve best practice compliance. Each agency shall manage its own risk through this process in accordance with the Information Technology Risk Management Policy with Guidelines. In agencies with more than 50 employees, the process shall include a review committee, with at least one member being a security specialist[14]. The process methodology shall incorporate an approach to block all ports then permit specific ports which have a business requirement access while incorporating additional hardening as necessary to have a comprehensive security policy. For temporary or emergency port openings, the agency process shall establish a maximum time for the port to be open, which shall not exceed 15 days. The agency committee, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.

2. Identity: System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.

3. Physical Security Firewalls shall be installed in locations that are physically secure from tampering. The agency security information technology liaison shall approve the physical location of the firewalls. Firewalls shall not be relocated without the prior approval of the IT security liaison.

4. Firewall Rulesets Firewall rulesets shall always block the following types of network traffic[15]:

    - Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.

[13] The Firewall Configuration Standard has been added at the end.

[14] A security specialist for firewall configuration is an individual who understands firewall technology and security requirements. If ITS manages the firewall, ITS will provide the security specialist.

[15] Exceptions to the blanket rules are included in the applicable bullets.

- Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.
- Traffic inbound to the State Network containing ICMP (Internet Control Message Protocol) traffic will be blocked at the perimeter with the following exceptions: To allow testing initiated from internal IT support groups, ICMP echo replies and ICMP TTL expired will be permitted inbound to the State Network but will be limited to specific IP addresses or small subnets representing the internal support group. A ping point can be established at the perimeter, for troubleshooting purposes, with the sole purpose and sole capability of responding to a ping. ~~Inbound network traffic containing ICMP (Internet Control Message Protocol) traffic. PING may be allowed.~~
- Inbound network traffic containing IP Source Routing information
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0
- Inbound or outbound network traffic containing directed broadcast addresses.

5. Minimum Firewall Requirements:
   - ~~No~~ Local user accounts shall be configured on network firewalls, for the sole purpose of eliminating possible extended outages. Local accounts shall be configured to only become active when the device can not make contact with the central unit. During normal operation, the local account exists but is unusable. Firewalls must use an authentication mechanism that provides accountability for the individual.
   - Passwords on firewalls shall be kept in a secure encrypted form.
6. Monitoring and Filtering
   - Logging features on state network firewalls shall capture all packets dropped or denied by the firewall, and agency staff or the entity managing the firewall, such as ITS, shall review those logs at least monthly.
   - Each agency's firewall policy shall be reviewed and verified by agency staff at least quarterly. If an outside entity, such as ITS, manages the firewall, then that entity shall be responsible for reviewing and verifying the agency's firewall policy at least quarterly.

ISO 27002 References
11.4.7 Network routing control

030503 Managing Databases

Purpose: To protect the State's information databases.

STANDARD[16]

Agencies shall properly safeguard the confidentiality (where applicable), integrity and availability of their databases. Data from these databases shall be protected from unauthorized deletion, modification or misuse and shall meet all applicable statutory and regulatory requirements.

Critical data files shall be backed up, and if confidential data is backed up, the backup media shall receive appropriate security controls.

[16] Section 3.1.8 of the Desktop and Laptop Security Standard has been added.

GUIDELINES

To maintain the reliability of databases maintenance must be performed on the operating system of the system that hosts the databases, or there is a greater possibility that the database itself will fail.

Databases that store critical, confidential information such as client records, accounting data, medical history data and data on sales and purchases should require more stringent mean time between failures (MTBF) and mean time to repair (MTTR) configurations.

ISO 27002 References
12.2 Correct processing in applications
15.1.3 Protection of organizational records

050103 Installing New Hardware and Software

Purpose: To ensure that new hardware and software is subjected to operational and security review prior to installation.

STANDARD[17]
Agencies involved with the installation of new hardware shall establish a formal review process that allows entities affected by the new hardware to review and comment on the implementation plans and the operational and security requirements.

The review process shall include, but not be limited to, the following:

- Notification of all impacted parties prior to the installation of new hardware.
- Circulation to appropriate individuals of planned changes or disruptions to operational status or information security for the new installation.
- Installation of equipment in an appropriately secured and environmentally controlled environment.
- Restricting access to the proposed changes (i.e., network diagrams, security features, locations, configurations, etc.) to those who require the information to perform their job duties.
- Performing a risk analysis on the hardware installation process, including possible worst-case scenarios.

Only standard approved software shall be installed on desktops and laptops with any deviations being pre-approved by agency management and review by a security administrator assigned to perform the review.

Default settings for applications such as e-mail calendar, and Internet access tools must be set to support a secure environment.

Security reviews shall be performed internally on a regular basis to ensure compliance with the standard requirements.

ISO 27002 References
12.1.1 Security requirements analysis and specification

[17] Sections 3.1.09, 3.1.10, and 3.1.11 of the Desktop and Laptop Security Standard have been added

050204 Using Modems/ISDN/DSL Connections

Purpose: To protect confidential information being transmitted over public networks[18].

STANDARD[19]

No modems shall be used on desktop and laptop computers, except as specifically authorized by the agency security administrators.

Agencies using modem (cable or telephone)/ISDN/DSL connections to transmit confidential information over public networks shall implement the following security measures to prevent disclosure of the confidential information:

- The agency shall require personnel to encrypt or transmit through a secure connection such as VPN or SSL all confidential information, including user passwords and Social Security numbers, to protect the confidentiality and integrity of the information.
- The agency shall require those who transmit information via these types of connections to notify the intended recipient that the information is being sent.

ISO 27002 References
10.8.5 Business information systems

SECTION II – Changes to Existing Standards

The standards in this section reflect minor changes to update and/or clarify existing standards. Because of the increasing use of Virtual Machines (VMs), language has been added to remind users that, in general, VMs require the same security as physical operating systems.

020115 Access Control Framework

Purpose: To establish standards for Agencies accessing the State network.

STANDARD

Agencies shall follow the attached matrix, Security Framework Template, to prevent unauthorized access to information systems. Agencies shall use appropriate placement and configuration that provides protective measures that are commensurate with the security level required to protect the data contained in those systems.

Agencies shall assess the risk associated with each business system to determine what security rules apply to the system and/or application. The security assessment determines the appropriate placement of each system and application within the security

[18] For the purpose of this standard, public network includes the State Network.

[19] Section 3.1.04 from the Desktop and Laptop Security Standard has been added

framework and evaluates the network resources, systems, data and applications based upon their criticality. The assessment assigns correlative security requirements. As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase.

Security Requirements

Security for the network infrastructure and for distributed systems operated by state agencies shall comply with the security requirements of the template, which is attached and is expressly made part of this policy. All executive branch agencies capable of meeting the security requirements for the Demilitarized Zone (DMZ) and/or Secure Zone as listed in the template shall do so.

Special Assembly Security Requirements

Agencies not able to adhere to the DMZ and/or security requirements shall develop a Special Assembly zone and document the rationale for developing the Special Assembly zone. Security controls in the Special Assembly area are not as structured as controls in the DMZ/Secure zones. Agencies acknowledge that additional security risks are associated with the Special Assembly zone.

Virtual Environment Requirements

Virtual machines are located on physical machines. As such, virtual machines shall use the same security controls as physical machines, and the virtual environment shall use secure communication and network zoning as the physical environment does (See the Security Framework matrix below)[20]. Virtual machines shall also be separated by functionality, content, and risk. Higher risk virtual machines must not share the same physical host as lower risk virtual machines.

030102 Managing the Networks

Purpose: To establish a framework for the management and protection of the State's network resources.

STANDARD

Agencies' network infrastructure shall be managed using controls to safeguard the State's information systems. Failure to protect against threats can result in loss of data integrity, data unavailability and/or unauthorized use of data.

Secure management of the network infrastructure shall include but not be limited to the following:

- Use of secure protocols such as Secure Shell (SSH), Secure Sockets Layer (SSL), Internet Protocol Security (IPSec), Simple Network Management Protocol (SNMP) version 3, etc., for network management.

[20] The matrix is not included here. To review it, refer to Standard 020115 in the Statewide Information Security Manual at http://www.scio.state.nc.us/documents/docs_Active/Statewide%20Information%20Security%20Manual/Combined%20Approved%20Chapters%20of%20Security%20Manual.pdf

- Employ secure protocols within virtual environments for network communications between virtual machines, between virtual machines and the host OS, and between virtual machines and the physical server.
- Use of authentication, authorization and accountability mechanisms when administering network devices.
- Monitoring for attempts to deny service or degrade the performance of information systems (including computers, microcomputers, networks, telephone systems and video systems).
- Restriction of transfers of large amounts[21] of data between computing systems during business hours, unless required or authorized by senior management.
- Definition of tasks/roles/responsibilities involved in management and security of agency IT resources in job descriptions.

ISO 27002 References

8.1 Prior to employment
10.6.1 Network controls
11.4.1 Policy on use of network services
11.4.2 User authentication for external connections

030203 Controlling Data Distribution and Transmission

Purpose: To protect the State's data and information from unauthorized disclosure.

STANDARD

Technical access controls or procedures shall be implemented to ensure that data and information are distributed only as authorized and as appropriate. Access controls and/or procedures shall, in part, be based on agency business requirements. Once a business justification is provided, personnel shall adhere to the following standards:

- If information includes both confidential data and data available for public inspection, the classification level shall default to confidential.
- Electronic media entering or leaving offices, processing areas or storage facilities shall be appropriately controlled.
- Storage areas and facilities for media containing confidential data shall be secured and all filing cabinets provided with locking devices.
- Confidential information shall not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements, and return dates.
- When confidential information is shipped, the delivery shall be verified.
- All confidential information shall be encrypted when transmitted across wireless or public networks[22] including transmissions such as FTP or electronic mail.
- Encryption algorithms for the transmission of confidential data include, at a minimum, Secure Socket Layer (SSL) RC4 128 bit algorithms, SSL Server-Gated Cryptography (SGC) 128 bit algorithms, TLS 1.11 128 bit algorithms, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST)[23].

[21] Because each service and network is different and because bandwidth capabilities differ, "large amounts of data" must be a subjective term.

[22] For the purpose of this standard public network includes the State Network.

[23] NIST http://csrc.nist.gov/groups/STM/cavp/index.html

ISO 27002 Reference
9.1 Secure Areas

030303 Sending Electronic Mail

Purpose: To establish requirements for sending electronic mail.

STANDARD

Agencies shall develop policies regarding unacceptable use of email and set forth the extent to which users may use agency-provided email for personal use. Agencies that connect to the State Network are subject to the statewide acceptable use policies.

Examples of email content that constitute unacceptable use are:

- Private or personal for-profit activities. This includes personal use of email for marketing or business transactions, advertising of products or services or any other activity intended to foster personal gain.
- Unauthorized not-for-profit business activities.
- Use for, or in support of, unlawful/prohibited activities as defined by federal, State and local laws or regulations. Illegal activities relating to Internet and network access include, but are not limited to:
- Tampering with computer hardware or software.
- Knowingly vandalizing or destroying computer files.
- Transmitting threatening, obscene, or harassing materials.
- Attempting to penetrate a remote site/computer without proper authorization.
- Using the Internet in an effort to access data that are protected and not intended for public access.
- Violating federal and State laws dealing with copyrighted materials or materials protected by a trade secret.
- Intentionally seeking information about, obtaining copies of or modifying contents of files, other data or passwords belonging to other users, unless explicitly authorized to do so by those users.
- Sending confidential information without encrypting that information, exposing the data to discovery by unintended recipients.
- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
- Deliberate interference or disruption of another user's work or system. Users must not take actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance) or the introduction of computer worms or viruses by any means.
- Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities.
- Unauthorized distribution of State data and information.
-

ISO 27002 References
10.8.2 Exchange agreements
10.8.4 Electronic messaging
12.2.3 Message integrity

030603 Managing Backup and Recovery Procedures

Purpose: To ensure recoverability and availability of the State's information technology resources.

STANDARD

Agencies shall manage the backup and recovery procedures of their information technology systems according to their business continuity plans. These plans must be properly documented, implemented and tested to ensure operational viability and their adherence to N.C.G.S. §147-33.89.

GUIDELINES

In managing backup and recovery procedures, agencies should consider the following: ~~establishing requirements that:~~

- Backup schedules meet business system requirements.
- Backup and restoration processes are tested on a regular basis.
- Backup facilities are adequate for minimum levels of operation.
- Retention periods of various data are based on operations, laws and regulations.
- Backup and recovery procedures are periodically reviewed and updated, as necessary.
- Validate the integrity of the backup or image file through file hashes for backups, restores, and virtual machine migrations.

RELATED INFORMATION

Standard 140101	Initiating the Business Continuity Plan
Standard 140102	Assessing the Business Continuity Plan Risk
Standard 140103	Developing the Business Continuity Plan
Standard 140104	Testing the Business Continuity Plan
Standard 140105	Training and Staff Awareness on the Business Continuity Plan
Standard 140106	Maintaining and Updating the Business Continuity Plan

ISO 27002 Reference
10.5.1 Information back-up

030801 Using Encryption Techniques

Purpose: To protect the State's confidential information using encryption techniques.

STANDARD

Each agency shall document and retain on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its unencrypted transmission to a ~~third~~ party not served by the agency's internal network. ~~State Network~~. Encryption techniques shall be employed when encryption is appropriate.

Since a virtual machine image file contains the entire virtual machine (server and all data), agencies ~~should~~ shall consider securing virtual machine image files using encryption technologies, particularly where the image file is backed up to another storage media outside of the agency's control.

All portable computing devices, including laptops and other mobile computing devices such as personal digital assistants (PDAs) and portable media such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct the public's business~~,~~ shall use encryption to protect all information, including confidential information~~, including~~ such as personal information, from unauthorized disclosure.

Agencies using key-based encryption systems must provide for an encryption key escrow to ensure present and future agency access to encrypted data. Agencies must ensure that only authorized personnel have access to keys used to access confidential information.

Proper management control of encryption keys and processes must be ensured when archiving confidential electronic files or documents.

Device	Encryption Requirements
Laptop and Notebook	Full Disk (sector-level) - FIPS 140-2 Level 1 certified AES-256 encryption algorithm.
Removable Media such as CDs, memory sticks and, DVDs, or any other portable device that stores data.	Data encrypted using FIPS 140-2 Level 1 certified AES-256 algorithm. Where possible, full disk encryption shall be used. File, volume, or virtual disk encryption may be used to store confidential data when full disk encryption is either not applicable or not possible. Encrypted files containing confidential data shall not be decrypted to removable media. Where possible, government confidential data shall be stored on state issued and owned removable media.
Tape Media	All portable tape media that could contain confidential information, that may be transported or stored off-site, must be encrypted. Agencies should use an encryption algorithm of, at a minimum, 128-bit strength.
Hand-Held Computing Devices, such as smart phones, Blackberries and Blackberry-like devices, and PDAs.	Confidential data must be encrypted at a minimum using a FIPS 140-2 Level 1 certified AES-128 or Triple-DES encryption[2] algorithm. Where technically possible, full-disk encryption shall be used. File, volume, or virtual disk encryption may be used to store confidential data when full-disk encryption is either not applicable or not possible.

Agencies shall develop and enforce polices concerning the storage of the State's confidential data on all portable and removable media devices.

GUIDELINES

Agencies should consider encrypting all confidential information or data that would have an adverse impact on the agency's services or functions if their confidentiality were compromised.

Agencies should use an encryption algorithm of, at a minimum, 128-bit strength or one of those accepted and approved by the National Institute of Standards and Technology.

Due to the greater likelihood for theft or loss, users should be instructed to avoid storing confidential information on portable media and devices whenever possible.

For satellite locations, or for locations where weaker physical access controls are present, agencies should strongly consider deploying full-disk encryption on desktops that store confidential information.

Since a virtual machine image file contains the entire virtual machine (server and all data), agencies should consider securing virtual machine image files using encryption technologies, particularly where the image file is backed up to another storage media outside of the agency's control.

RELATED INFORMATION

Standard 010101	Setting Classification Standards—Defining Information
Standard 010102	Setting Classification Standards—Labeling Information
Standard 010103	Setting Classification Standards—Storing and Handling Information
Standard 010104	Setting Classification Standards—Isolating Top Secret Information
Standard 010105	Setting Classification Standards—Classifying Information
Standard 010106	Setting Classification Standards—Custodians of Confidential Information
Standard 010107	Setting Classification Standards—Managing Network Security
Standard 030203	Controlling Data Distribution and Transmission
Standard 030205	Managing Electronic Keys
Standard 030605	Archiving Electronic Files

ISO 27002 References
12.3.2 Key management
15.1.6 Regulation of cryptographic controls

030902 Loading Personal Screen Savers

Purpose: To protect the State's assets by eliminating non-approved screen savers.

STANDARD[24]

Personnel shall load only those screen savers that have been approved by their agencies.

Agencies shall train their employees on the risks of acquiring malware such as viruses, spyware and Trojan horses by downloading and installing unauthorized screen savers.

~~**GUIDELINES**~~

~~Personal screen savers can be resource intensive to computer systems. Agencies should strongly discourage downloading screen saver software from the Internet.~~

ISO 27002 References
10.4.1 Controls against malicious code

050402 Issuing Laptop/Portable Computers to Personnel

Purpose: To protect confidential data on laptop/portable computers and other handheld computing devices.

[24] The guideline is proposed for removal because it conflicts with the standard itself as well as Standard 050705 – Clear Screen.

STANDARD

Agencies shall authorize the assignment of portable personal computers to employees and require that users comply with all information technology security policies when using the portable devices, including the agency and statewide acceptable use policies, as applicable. Portable devices covered by this standard are those that connect to agency and State networks and/or store agency data and include:

- Laptop, notebook, and tablet computers.
- Handheld devices (electronic organizers, personal digital assistants [PDAs], Pocket PCs, etc.).
- Smart phones, Blackberries and Blackberry-like devices, cellular phones, pagers, and other mobile communication devices.
- Flash drives and thumb drives, CDs, and other portable storage devices or removable media.

GUIDELINES

Agency management should consider using the following additional security controls, as appropriate:

-
  - Check-in procedures for portable devices that verify that the device is free of unauthorized software, viruses, or any other malicious code prior to reissue or reconnection to the network.
  - Training to raise user awareness of the additional risks that accompany mobile computing and the controls with which users must comply.

RELATED INFORMATION

Standard 050403 Using Laptop/Portable Computers

ISO 27002 References

11.7.1 Mobile computing and communications

050403 Using Laptop/Portable Computers

Purpose: To promote the secure use of laptops and other portable devices.

STANDARD

Agencies shall implement appropriate safeguards to ensure the security of laptops and other portable computing devices. Specifically:

- Portable computing devices shall:
-
  - Adhere to the mobile data encryption standard[25] if technically possible.
  - Be physically secured when the users have taken them out of a secure area.
  - Be labeled with tamper-resistant tags identifying the device as property of the State, a permanently engraved serial number or both.

[25] Standard 030801 Using Encryption Techniques

- Comply with all applicable security requirements for desktops.
- The BIOS password on such devices, if applicable, must be enabled.
-

- If not protected by encryption software, the BIOS password on such devices must be enabled if technically possible.

- When a laptop is outside a secure area, data on the laptop must be backed up, and the backup must be kept separate from the laptop.

GUIDELINES

The small size and mobility of portable computing devices are the primary causes of the attendant security risks. Information security controls that agencies should consider include, but are not limited to, the following:

- Procedures governing appropriate use of portable devices in unprotected areas (meeting rooms and off-site locations).
- Restricting use of such devices via a wireless connection that originates from anywhere other than State- or agency-approved networks.
- Training on how to physically secure devices against theft when left in cars or other forms of transport, hotel rooms, conference centers and meeting places.
- Training to raise user awareness of the additional risks that accompany mobile computing and the controls that should be implemented.

RELATED INFORMATION
030801 Using Encryption Techniques

050404 Working from Home or Other Off-Site Location (Teleworking)

Purpose: To secure and protect communications with agency information resources while personnel are working at off-site locations.

STANDARD

Personnel shall not work from home or off site using State-issued or personally owned computers or devices (commonly known as teleworking or telecommuting) unless authorized by agency management. Agencies that authorize teleworking for their personnel shall ensure the following:

- Agencies shall define standards for authorized personnel to securely access systems from off site. Standards shall include:

  - Use of agency-approved virus prevention and detection software.
  - Use of personal firewalls.
  - Securing home wireless networks.
  - Protecting portable electronic devices such as personal digital assistants (PDAs), Blackberries and Blackberry-like devices, and smart cell phones (combination PDA/cell phone/camera phones).

- Use of virtual private networking software or other technologies for protecting communications between off-site systems and agency information resources.
- Use of two-factor authentication products (such as one-time password tokens or biometric devices) to authenticate users, if applicable.
- Use of encryption products to protect data stored on off-site systems, if applicable.

- Agencies shall provide training to personnel for properly accessing systems from off site and for keeping antivirus software and personal firewall software up to date with the latest signature files and patches.

- Agencies shall also provide instructions and training for protecting confidential information transferred to, processed on or stored on non-State-issued systems, such as personal computers at home.

- Agencies shall document and retain evidence of training provided to a user during the time that the individual is authorized to access systems remotely.

Agency employees who are authorized to work from home shall ensure that the agency-defined standards for off-site work are strictly adhered to. Personnel shall take extra precautions to ensure that confidential information stored on personal computers or electronic devices is not divulged to unauthorized persons, including family members.

RELATED INFORMATION

Standard 020112	Controlling Remote User Access
Standard 030801	Using Encryption Techniques
Standard 050408	Day-to-Day Use of Laptop/Portable Computers

ISO 27002 References

9.2.5 Security of equipment off-premises
11.7.2 Teleworking

030405 ~~Giving Information When Ordering Goods on Telephone~~ Providing Confidential Information Over the Telephone

Purpose: To provide awareness that giving information over the telephone presents security risks

STANDARD

When confidential information (e.g., credit card number, social security number) is required while conducting business using the telephone, employees must ensure that they know exactly to whom they are speaking and whether that person is authorized to receive such information:

- Confidential information must not be left on answering machines or other recording devices.
-
- Care must be taken to ensure that confidential information cannot be overheard when it is disclosed over the telephone.
-

ISO 27002 References

10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030502 Managing Data Storage

Purpose: To protect the State's information resident on electronic data storage

STANDARD

Agencies shall ensure the proper storage of data and information files for which they are responsible. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse. Agencies shall also meet all applicable statutory and regulatory requirements for data retention, destruction, and protection.

The primary security control available to agencies to protect confidential data in storage is using a data encryption method approved by the State CIO. Care should be taken to ensure that encryption keys are properly stored (separate from data) for later decryption.

RELATED INFORMATION
Chapter 9 - Dealing with Premises Related Considerations

ISO 27002 References
10.7.3 Information handling procedures
15.1.3 Protection of organizational records

050403 Using Laptop/Portable Computers

Purpose: To promote the secure use of laptops and other portable devices.

STANDARD

Agencies shall implement appropriate safeguards to ensure the security of laptops and other portable computing devices. Specifically:

- Portable computing devices shall:
    - Be encrypted, if technically possible.
    - Be physically secured when the users have taken them out of a secure area.
    - Be labeled with tamper-resistant tags identifying the device as property of the State, a permanently engraved serial number or both.
    - Comply with all applicable security requirements for desktops.
- If not protected by encryption software, the BIOS password on such devices must be enabled if technically possible ~~applicable~~.
- When a laptop is outside a secure area, data on the laptop must be backed up, and the backup must be kept separate from the laptop.

GUIDELINES

The small size and mobility of portable computing devices are the primary causes of the attendant security risks. Information security controls that agencies should consider include, but are not limited to, the following:

- Procedures governing appropriate use of portable devices in unprotected areas (meeting rooms and off-site locations).
- Restricting use of such devices via a wireless connection that originates from anywhere other than State- or agency-approved networks.
- Training on how to physically secure devices against theft when left in cars or other forms of transport, hotel rooms, conference centers and meeting places.
- Training to raise user awareness of the additional risks that accompany mobile computing and the controls that should be implemented.
-
- RELATED INFORMATION

030801 Using Encryption Techniques

050408 Day-to-Day Use of Laptop/Portable Computers

Purpose: To promote the secure day-to-day use of laptop/portable computers.

STANDARD

Personnel who use an agency laptop/portable computer shall ensure that the laptop/portable computer and the information it contains are suitably protected at all times.

~~Where technically possible, a~~ Agencies shall require that laptops~~ and other State issued mobile electronic devices~~ have:

- Full disk encryption.
- Locks.
- ~~BIOS password protection~~
- ~~Cryptographic capabilities for confidential information.~~
- Regular backups.
- Current antivirus software.
- Firewalls configured to comply with State and agency policies.

Where technically possible, agencies shall require that other mobile electronic devices used for conducting the state's business comply with the same standards as laptops. Where full disk encryption is not technically possible, mobile electronic devices shall have other protection mechanisms such as BIOS password or PIN access.[26]

Agencies shall periodically audit these devices to ensure compliance with these requirements.

[26] For hand held devices (e.g. smart phones, personal data assistants, and Blackberry-like devices) that connect to the State Network, see 020112 Controlling Remote Access.

ISO 27002 References
11.7.1 Mobile computing and communications

060104 Defending Against Premeditated Internal Attacks

Purpose: To limit the potential damage caused by internal attacks.

STANDARD

To defend against insider attacks on agency networks and to prevent internal damage, access rights to files shall be controlled to maximize file integrity and to enforce separation of duties.

- Access to files shall be granted only on as required for the performance of job duties.
- Networks that serve different agencies or departments shall be segregated, and access to those segmented networks shall be established as appropriate through the use of VLANs, routers, firewalls, etc.
- In a distributed computing environment, virtual machines should be separated by functionality and/or content. High risk virtual machines should not share the same physical server with low risk virtual machines. A physical server should also not host virtual machines located in different security zones.
- Access badges shall be programmed to allow entry only into assigned places of duty.
-
- Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and Trojan code.
-
- Users' activities on systems shall be monitored to ensure that users are performing only those tasks that are authorized and to provide an appropriate audit trail.

ISO 27002 REFERENCES
10.10.2 Monitoring system use
11.1.1 Access control
11.6.1 Information access restriction

140103 Developing the BCP

Purpose: To require that the appropriate level of information technology business continuity management is in place to sustain the operation of critical information technology services to support the continuity of vital business functions.

STANDARD

Management shall develop a business continuity plan (BCP) that covers all of the agency's essential and critical business activities and that includes references to procedures to be used for the recovery of systems that perform the agency's essential and critical business activities.

At a minimum, an agency's business continuity plan shall:

- Help protect the health and safety of the employees of the State of North Carolina.

- Protect the assets of the State and minimize financial, legal and/or regulatory exposure.
- Minimize the impact and reduce the likelihood of business disruptions.
    - Crisis teams and response plans for threats and incidents.
    - Communication tools and processes.
- Require that employees are aware of their roles and responsibilities in the BCP and in plan execution.
    - Training and awareness programs.
    - Simulations and tabletop exercises.
- Have a documented policy statement outlining:
    - Framework and requirements for developing, documenting, and maintaining the plans.
    - Requirements for testing and exercising.
    - Review, sign-off and update cycles.
    - Have senior management oversight and sign-off.
    - Assess the professional capability of third parties and ensure that they provide adequate contact with the agencies.
    - Review dependence on third parties and take actions to mitigate risk associated with dealing with third parties.
    - Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.
    - Set forth procedures to be followed for restoring critical systems to production.

The State CIO shall determine the format, timing and other details for submission of the reports.

ISO 27002 REFERENCES

14.1.03 Developing and implementing continuity plans including information security
14.1.04 Business continuity planning framework

SECTION III – Additional Policy Updates

This section includes updates to two policies that are not included in the Statewide Information Security Manual *per se* but are part of an appendix to the Manual: (1) Information Technology Risk Management Policy with Guidelines; and (2) the Electronic Mail Server Security Standard. Other existing security policies included in the appendix are:

- Application Security with Guidelines; and,
- Enterprise Authentication and Authorization Services Policy

Information Technology Risk Management Policy with Guidelines

Purpose: To ensure that state agencies manage risks appropriately. Risk management includes the identification, evaluation, and control of risks associated with an agency's business, information technology infrastructure, the information itself, and physical security to protect the state's information technology assets and vital business functions.

Scope: This policy applies to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services.

POLICY STATEMENT

The State of North Carolina recognizes that each agency, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to the state's citizens. The risk management program must identify and classify risks and implement risk mitigation as appropriate. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.

GUIDELINES

Agencies are encouraged to select and use guidelines that support industry best practices for risk management relative to business continuity planning and security as appropriate. Some suggested guidelines are listed below.

Risk Management Program Activities:

Agency risk management programs should focus on the following four types of activities:

- **Identification of Risks:** A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.
- **Analysis of Risks:** An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.
- **Mitigation Planning:** Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For important risks, mitigation plans should be developed.
- **Tracking and Controlling Risks:** Collecting and reporting status information about risks and their mitigation plans, responding to changes in risks over time, and taking corrective actions as needed.

Business Continuity Risk Management Processes: For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt agency business. Agencies should identify the potential impacts in order to develop the strategies and justify the resources required to provide the appropriate level of continuity initiatives and programs.

Agencies should conduct business risk impact analysis activities that:

- Define the agency's critical functions and services.
- Define the resources (technology, staff, and facilities) that support each critical function or

service.

- Identify key relationships and interdependencies among the agency's critical resources, functions, and services.
- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.
- Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Estimate financial losses over time of each critical function or service.
- Estimate tangible (non-financial) impacts over time of each critical function or service.
- Estimate intangible impacts over time of each critical function or service.
- Document any critical events or services that are time-sensitive or predictable and require a higher-than-normal priority. (For example - tax filing dates, reporting deadlines, etc.)
- Identify any critical non-electronic media required to support the agency's critical functions or services.
- Identify any interim or workaround procedures that exist for the agency's critical functions or services.
- Ensure adequate preparations for backing up critical applications.

Security Risk Process: The focus of security risk management is an assessment of those security risk outcomes that may jeopardize agency assets and vital business functions or services. Agencies should identify those impacts in order to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical agency functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize agency critical functions and services.

Security risk impact analysis activities include the:

- Identification of the federal, State, and local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for agency functions or services.
- Identification of any due diligence requirements for agency functions or services.
- Identification of confidential information stored in the agency's files and the potential for fraud, misuse, or other illegal activity.
- Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical agency functions and services.
- Identification of the processes used to monitor and report to management on the IT Security infrastructure. (Baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.)
- Identification of the agency's IT Change Management and Vulnerability Assessment processes.
- Identification of what security mechanisms are in place to conceal agency data (Encryption, PKI, etc.)

Electronic Mail Server Security Standard

Scope: The standard applies to all state agencies, departments, institutions, commissions, committees, boards, divisions, bureaus, offices, officers, and officials of the State, except for the General Assembly, the Judicial Department, or The University of North Carolina and its constituent institutions, unless they elect to participate in the information technology programs, services, or contracts offered by the Office of Information Technology Services (ITS).

1.0 Rationale[27]

To reduce unauthorized access to electronic mail (e-mail) systems by requiring security measures that are commensurate with the risks attendant to such systems.

2.0 Enterprise Wide Standard

All e-mail services offered or subscribed to by state agencies subject to G.S. §147-33.110 must adhere to the security requirements of this standard.[28]

2.1 Configuration

1. All services and operations shall be disabled except those which are expressly permitted (*e.g.,* Web based mail, FTP, remote administration) and only the minimal Internet services required shall be installed.

2. Default accounts and groups shall be disabled or removed.

3. The service banner shall not report the mail server and operating system type and version.

4. The mail server shall be configured to use encrypted authentication of passwords or other authentication data.

.

5. All mail servers used to relay mail, e.g., via the SMTP protocol from email client software, shall be configured to only accept email from authenticated sources.[29]

6. All servers used to receive email, e.g., from external sources via the SMTP protocol, shall be configured to only accept incoming mail for email domains they represent.

7. All mail servers where possible shall not allow the "from," or alternative standard return header, to be an email address domain that it does not represent

8. All mail servers used to relay mail shall be configured to rate limit message delivery to within acceptable performance standards to reduce successful Denial of Service (DoS) attacks.

---

[27] This standard is primarily based upon principles set forth in NIST Special Publication 800-45, Version 2 (2007) "Guidelines on Electronic Mail Security".

[28] E-mail services also must comply with other security standards and policies, including the User ID and Password Protection Standard and Virus Protection Policy with Guidelines.

[29] This can be achieved by login credentials sent over an encrypted connection or by connection from specific IPs before the server accepts the mail to be sent.

9. Any mail transport agent (MTA) server software used solely for the purpose of allowing a local application to send emails, e.g., monitoring software that sends alerts via SMTP, shall be installed and configured so that:

    - Its only function is to send, not receive email.
    - It can only send to the host(s) whose function(s) is(are) the primary mail server for the agency.
    - It accepts connections only from the host it is installed on, eg., via localhost or socket.
    - It has a valid sending email address that can accept bounces if any.
    - Where possible, the server shall not allow the "From" or alternative standard header to be an email address domain that it does not represent.

2.2 Mail Server

A mail server shall be on a dedicated, single-purpose host, whether it is a physical server or a virtualized server. The server shall have a dedicated physical disk or logical partition for mailboxes (separate from the operating system and server application).

All mail commands which can be used to obtain information on accounts, or are otherwise unnecessary or dangerous, that are not required for normal operation (*e.g.,* VRFY and EXPN) shall be disabled.

All mail servers shall use a file integrity checker to monitor changes to critical files on the mail server (host-based or file-integrity checker)[30]

2.3 Firewall/Mail Relay

1. The mail server shall be protected by a firewall that controls all traffic between the Internet and the server.

2. Incoming and outgoing messages shall be scanned for viruses at the firewall or mail relay. If attachments are allowed on the e-mail service, the mail server administrator shall filter potentially dangerous attachment types (*e.g.*, .exe, .vbs, .ws, .wsc file extensions) at the mail server or mail gateway and conduct virus scans on allowed file types.

3. The firewall (or router that is acting as a firewall) shall block all access to the mail server from the Internet except those ports that are required to operate the e-mail server.

4. Where possible, the server containing the mailboxes shall be located in a secure zone separate from the server(s) whose function is to send/receive email, authenticates end users, and/or provides web-based access

2.4 Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

1. IDS/IPS shall monitor network traffic to and from the mail server.

[30] Some critical files will change regularly and, therefore, should not be protected by a file integrity checker. The determination of which files should be protected will depend on the mail server and the operating system used.

2. A firewall, in conjunction with IDS/IPS, shall block IP addresses or subnets that the IDS/IPS reports are attacking the organizational network.

3. IDS/IPS shall be configured to log events and the logs shall be maintained for at least three months. The retention of logs must also comply with any relevant legal and regulatory requirements, including the agency's records retention schedule.

4. IDS/IPS monitoring the mail server shall be updated with new attack signatures at least weekly.

2.5 Physical Security

E-mail servers and related items such as communication wiring and networks shall be located in secure locations that are locked and restricted to access by authorized personnel only.

GUIDELINE

When evaluating upgrades to e-mail servers, the inclusion of technology allowing electronic signatures for signing messages for sender validation should be considered.

SECTION IV – Glossary

The changes and additions to the Statewide IT Glossary are below. The link to the Statewide IT Glossary is:
http://www.scio.state.nc.us/documents/docs_Active/Statewide%20Information%20Security%20Manual/Glossary%20of%20Terms.pdf

Backup – ~~The process of making a duplicate copy of data on a computer's hard disk.~~ The process of duplicating data stored on a computer's hard disk to another storage medium for the purpose of system and/or data restoration to its original state following a disaster or other inadvertent loss. Backup may also refer to alternative processing capabilities through secondary systems.

Critical Data Point – See Recovery Point Objective.

Hypervisor / Host OS – a virtualization platform that allows multiple operating systems to run on a host computer at the same time. Also called a Virtual Machine Monitor.

.

Confidentiality – Written ~~C c~~ommunication conducted in confidence of secrecy, as authorized by State and federal laws.[31]

Mesh Networking – A way to route data between nodes employing one of two connection arrangements: *full mesh* topology or *partial mesh* topology. In the *full mesh* topology, each node is connected directly to each of the others. In the *partial mesh* topology, some nodes are

[31] *See,* News and Observer Publishing Co. v. Poole, 330 N.C. 465, 474, 412 S.E.2d 7, 12 (1992); and G.S. §132-6.1(c).

connected to all the others, but some are connected only to those other nodes with which they exchange the most data. One advantage of a mesh network is that it offers redundancy. If one node can no longer operate, the rest can still communicate with each other, directly or through one or more intermediate nodes.

North Carolina Integrated Information Network (NCIIN) – A retired term that refers to a web of interoperable networks, within the state, that transmits data, text, images, voice, and video. The NCIIN is now called the State Network.

Personal Computing Device – Any device, including a PDA, laptop, Blackberry-like device, or smart phone that can store and process data.

Portable Storage Device – *See, Removable Media.*

Recovery Point Objective (RPO) – The point in time to which systems and data must be recovered following an adverse event, *e.g.* the last completed transaction or the point immediately before the last backup commences. Also known as the Critical Data Point.

Recovery Time Actual (RTA) – The time frame that technology support staff actually takes to deliver the recovered infrastructure to the business. The RTA is usually determined during tests.

Recovery Time Objective (RTO) – The duration of time and a service level within which systems, applications, or functions must be restored after an outage to the predetermined Recovery Point Objective (RPO), for example, one business day.

Removable Media - Electronic storage devices that can be used to store and/or move data between computing equipment. Removable media includes electronic storage media such as floppy disks, compact discs, DVDs, portable USB thumb drives, external hard drives, and flash memory cards.

Virtual Machine for Operating Systems – In operating systems, the primary component of a virtualized architecture that serves to replace a traditional physical system or set of systems. Because VMs are separated from the physical resources they use, the host environment is often able to dynamically assign resources among the VMs.

The VM has a traditional OS installed within it that is called the guest OS. This guest OS communicates with the Virtual Machine Monitor (VMM) which manages the interaction of the OS with the hardware. One of the key characteristics of most VMs is that they operate exactly like their physical counterparts so that not only do users experience the same look and feel, but also the system's software programs do not recognize that they are operating within a VM.

Virtual Machine Monitor – A component of a virtualized environment that performs the intelligent processing of a virtualization solution. It operates between the Virtual Machine (VM) and the hardware and performs the translation between the software in the VM and the low-level device drivers. If the virtual machine monitor (VMM) provides all of the virtual machine process and has all of the device drivers, it is also called a "hypervisor." If it uses a guest operating system to provide the device drivers, the VMM is made up of that guest operating system (service level operating system) and a "micro-hypervisor." In both situations, the hypervisor is the closest to the hardware.

Virtual Network – An interconnected group of virtual machines configured to use a network adapter in the physical computer or no network adapter.

Virtual Switch – The network conduit among the virtual network interface cards of a Virtual Machine (VM), other VMs on the same physical host, and the physical network where it binds to

the physical network interface cards (NICs) on a machine. The Virtual Switch provides the same services as a physical switch. Every VM that is configured for network communications has a virtual network device driver that sends packets to the virtual switch.

Wireless Mesh Network – A wireless mesh network (WMN) provides communication between nodes over multiple access points (AP) on a full or partial mesh topology. In an infrastructure mesh configuration, the WMN uses wireless links (peer radio devices that don't have to be wired to a wired port like traditional APs do) to provide a data path from unwired fixed access points to other unwired APs or back to an access point that has a connection to a wired network. The nodes basically act as routers, using a wireless mesh routing protocol to establish frame-forwarding paths through the mesh.

SECTION IV – Removal of SLAs from Standards

ITS uses the ITIL process for its management of services offered to agencies and calls the service descriptions SLAs. In the Statewide Information Security Manual, SLAs have been considered contracts. To avoid confusion, all references to SLAs were removed and replaced with the word "contract."